Machine Learning in Penetration Testing

HUỲNH NGUYỄN UYỂN NHI, TRẦN MINH DUY, and PHẠM NGỌC THIỆN

ACM Reference Format:
Huỳnh Nguyễn Uyển Nhi, Trần Minh Duy, and Phạm Ngọc Thiện. 2024. Machine Learning in Penetration Testing. 1, 1 (June 2024), 1 page. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 GIỚI THIỆU ĐỀ TÀI

Penetration Testing (hay PT) là kỹ thuật kiểm thử xâm nhập và phát hiện lỗ hổng thông qua việc mô phỏng các tấn công của hackers để khai thác thông tin giá trị trong network, applications, database, v.v. Tuy nhiên việc kiểm thử xâm nhập bằng tay truyền thống thì tốn khá nhiều thời gian, và một số quy trình đòi hỏi các chuyên gia bảo mật đưa ra quyết định phù hợp. Đặc biệt trong những phạm vi lớn (eg: large networks) thì PT thực hiện càng phức tạp, tốn thời gian, và có xu hướng lặp đi lặp lại.

Nghiên cứu này tập trung phân tích và hiện thực việc tích hợp machine learning (ML) cụ thể là Reinforcement Learning với pentest nhằm giảm độ phức tạp, tiết kiệm thời gian và tự động hóa việc đưa ra quyết định.

2 LÝ DO NGHIÊN CỨU ĐỀ TÀI

Hệ thống mang lỗi tiềm ẩn hoặc xảy ra lỗi không rõ nguyên do là chuyện không nên xảy ra, gây hậu quả vô cùng nghiêm trọng. Do đó việc Pentest hệ thống ngày càng được chú trọng để phát hiện các lỗ hổng và đưa ra biện pháp khắc phục kịp thời trước khi tấn công thực sự diễn ra.

Việc tự động hóa pentest có nhiều thách thức: kiến thức, phương pháp, state space và action space lớn và rời rạc. Các ứng dụng RL vào pentest chỉ mới cho thấy hiệu quả trên một số trường hợp lý tưởng trong môi trường ảo.

Trong nghiên cứu này, nhóm tôi thực hiện phân tích và hiện thực một số mô phỏng dùng RL trong ngữ cảnh CTF đơn giản, với mục đích là tự động hóa quá trình đưa ra quyết định, đồng thời áp dụng các kỹ thuật để tối ưu hóa việc học của thực thể.

3 HƯỚNG NGHIÊN CỨU LIÊN QUAN

Bài báo áp dụng Q-learning để giải quyết các mô phỏng liên quan đến 3 loại CTF challenges thường gặp: Port Scanning and Intrusion, Server Hacking, và Website Hacking. Việc mô hình hóa các CTF challenges như sau:

- Agent: Đóng vai trò là pentester trong PT, học cách tấn công hệ thống thông qua các hành động và phản hồi.
- Môi trường: Hệ thống server mà agent tương tác.
- Action: những hành động attacker có thể dùng để khai thác: scan, exploit, get flag ...
- State: trạng thái server ở thời điểm cụ thể.
- Reward: được điểm hay trừ điểm ở mỗi lượt tương tác.

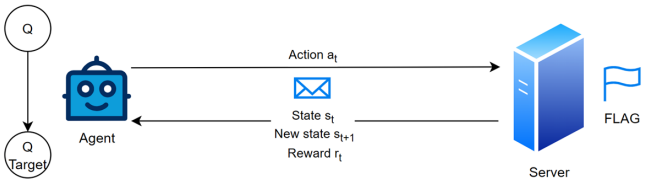

Fig. 1. Our formalism in modeling CTF challenges as RL problems.

Đồng thời, áp dụng các kỹ thuật: Lazy loading, State Aggregation, Imitation learning để tối ưu tốc độ học của agent.

4 NỘI DUNG DỰ KIẾN

- Tìm hiểu về RL/DRL và quy trình Pentest cơ bản trong thực tế.
- Phân tích bài báo.
- Tìm hiểu tổng thể về từng simulation và kỹ thuật áp dụng Lazy loading, State Aggregation, Imitation learning.
- Tái thực nghiệm lại từng simulation và đánh giá kết quả thực nghiệm của nhóm.
- Phát triển thêm một simulation áp dụng cả 3 kỹ thuật Lazy loading, State Aggregation, Imitation learning để nâng cao tối độ học.
- So sánh kết quả với bài báo và rút ra kết luận

Authors' address: Huỳnh Nguyễn Uyển Nhi, 21522424@gm.uit.edu.vn; Trần Minh Duy, 21522010@gm.uit,edu.vn; Phạm Ngọc Thiện, 21522627@gm.uit,edu.vn.

ACM XXXX-XXXX/2024/6-ART
https://doi.org/10.1145/nnnnnnn.nnnnnnn